International Journal of Teaching and Learning (INJOTEL) e-ISSN: 3025-8308
Vol. 1 No. 12, 2024, pages: 1486~1490

CYBER SECURITY EDUCATION PROGRAM FOR STUDENTS TO BUILD DIGITAL SECURITY AWARENESS

Agus Iskandar
Universitas Nasional, Jakarta, Indonesia
Correspondence author email: iskandaragus1005@gmail.com

Bagas Ade S
Universitas Nasional, Jakarta, Indonesia

Abstract

In the ever-evolving digital era, cyber security is a major concern, especially for the younger generation who spend significant time online. The Cyber Security Education Program for Students is designed to equip students with essential knowledge and skills in dealing with cyber security threats. Through a series of interactive workshops, training and simulations, this program aims to build awareness of the importance of digital security, teach how to identify and avoid various types of cyber attacks, and promote best practices in keeping personal and sensitive information safe. The program curriculum is structured based on the latest cybersecurity frameworks and delivered in a format that is easy for students to understand. The training material covers the basics of cyber security, such as password security, recognition of phishing, malware and ransomware, as well as self-defense techniques in cyberspace. In addition, this program also integrates the use of digital tools that can help students practice cybersecurity in their daily lives.

By participating in this program, it is hoped that students will become more aware and responsible in exploring the digital world, and be able to protect themselves and others from potential cyber security dangers. The Cyber Security Education Program for Students not only emphasizes the importance of cyber security knowledge and skills, but also encourages students to become digital security ambassadors in their environment, thereby creating a safer and more informed digital society.

Keywords: Cyber Security, Digital Security, Students, Educational Programs

INTRODUCTION

In the midst of accelerating digital transformation which affects various aspects of life, internet use by children and teenagers has increased significantly. Their existence in cyberspace opens up opportunities to learn, communicate and explore in ways that have never existed before. However, this also puts them at higher risk of various cybersecurity threats. From online fraud to cyberbullying to identity theft, digital security challenges continue to evolve and become more complex. Therefore, it is important for students to be equipped with the necessary knowledge and skills to deal effectively with these cyber threats.

Researchers obtained several supporting references, namely: according to (Yuliana, Y. 2022) thatThis program is good for improving cyber security among children to educate them to be aware of cyber threats and data theft. According to (Yustisia, KK, et

al 2023) that lDigital iteration is very important to be able to teach tostudents like to know about what information can and cannot be shared online and also the importance of the strength of passwords used on social media. According toTandirerung, VA, et al 2023) thatStudents can know the dangers of internet media and how to use internet media for positive and useful things. According to (Saputra, AF, et al 2024) thatthe importance of education regarding data or system security practices. According to (Nugroho, H., et al 2023) thatincrease awareness about cybercrime, especially phishing, in order to protect yourself from threats. According to (Alif, MS, et al 2021) thatlevel of security awareness of E-Wallet users in Indonesia based on demographic factors.

The Cyber Security Education Program for students aims to build digital security awareness among students, teach them about the importance of keeping personal and sensitive information safe, and arm them with practical skills to deal with and prevent cyber attacks. Through an interesting and age-relevant approach, this program aspires to create a young generation who is not only competent in using technology but also responsible and alert to potential cyber security risks.

Program activities include a series of workshops, interactive sessions, and simulations designed to strengthen understanding of cybersecurity among students. From a basic introduction to cyber security to best practices in maintaining online security, participants will be invited to understand and apply important concepts in digital security. By prioritizing active student participation, the Cyber Security Education Program for Students not only aims to increase knowledge but also change behavior, encouraging students to be part of the solution in facing cyber security challenges in the future.

RESEARCH METHODS

To evaluate the effectiveness of the Cyber Security Education Program for Students in building digital security awareness, this research will use a quantitative and qualitative approach. This method was chosen to gain a comprehensive understanding of the program's influence on participants' cybersecurity knowledge, attitudes and behavior. The following are the research methodology steps:

1. Research Design

This research will be conducted with a pre-experimental design using one pretest-posttest group. The participant group will have their knowledge of cyber security measured before and after participating in the program, to assess increases in knowledge and changes in attitudes and behavior.

2. Population and Sample

The population in this study were high school students who actively used the internet. The sample will be selected using a purposive sampling technique, with certain criteria relevant to the research objectives, such as age, internet use, and access to digital technology.

3. Data Collection

Qualitative data will be collected through in-depth interviews and focus group discussions (FGD) with participants, to gain deeper insight into their perceptions, experiences and feedback on the program.

4. Data Analysis

Qualitative data from interviews and FGDs will be analyzed using content or thematic analysis to identify key themes and patterns in participant responses. This will provide in-depth insight into the effectiveness of the program and how the program can be improved.

5. Validity and Reliability

To ensure the validity and reliability of the research instrument, the questionnaire will be tested on a small group before being widely implemented. Interviews and FGDs will be conducted by trained researchers to ensure consistency in data collection.

RESULTS AND DISCUSSION

Results

From the analysis of data collected through pretests and posttests, as well as interviews and focus group discussions (FGD), the research results show that the Cyber Security Education Program for Students has succeeded in increasing cyber security knowledge among participants significantly. Here are some key findings:

1. **Increased Knowledge**: Participants demonstrated an increase in the effectiveness of the educational material presented in increasing understanding of cyber threats and how to prevent them.
2. **Change of attitude**: Qualitative data analysis shows positive changes in attitudes towards cybersecurity practices. Participants are more aware of the importance of online security and more motivated to implement digital security practices in their daily lives.

Discussion

1. **Early Awareness as Key**: Building awareness about cyber security among students from an early age is key to developing safe online behavior. Effective education enables them to recognize and avoid cyber threats.
2. **The Importance of Relevant Content**: This research shows that educational content that is relevant to students' daily experiences is more effective in increasing understanding and encouraging behavior change.
3. **Active Role of Teachers and Parents**: Support from teachers and parents is needed to strengthen cybersecurity messages. Integrating cybersecurity into school curricula and home learning activities can increase the effectiveness of educational programs.

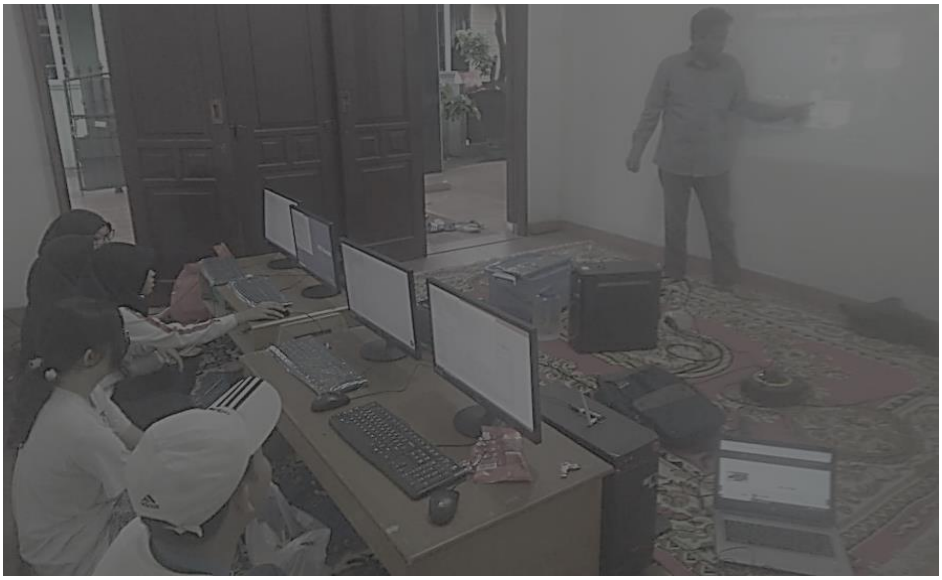

Figure 1. Educational activities being carried out

Overall, the Cyber Security Education Program for Students was successful in building awareness and increasing digital security among students. These findings underscore the importance of educational initiatives aimed at improving cybersecurity and empowering young people with the knowledge and skills to protect themselves in cyberspace.

CONCLUSION

The Cyber Security Education Program for Students has succeeded in showing a significant impact in building digital security awareness among students. Through a series of educational materials, interactive workshops and practical activities, this program not only increases participants' knowledge about cyber threats and how to prevent them but also succeeds in inspiring positive changes in cyber security attitudes and behavior. The results showed a marked increase in cybersecurity understanding, with participants being more careful in their online interactions and more proactive in implementing digital security practices.

This program has demonstrated that effective cybersecurity education requires an approach that is comprehensive and relevant to students' everyday experiences. By providing engaging and accessible content, and encouraging active participation from students, teachers, and parents, educational efforts can make a significant difference in reducing vulnerability to cyber threats.

In conclusion, the importance of cybersecurity in today's digital life cannot be underestimated, and effective cybersecurity education for students is a crucial step in preparing a generation that is safer and more responsible in cyberspace. The Cyber Security Education Program for Students is an example of how educational interventions can contribute positively to the development of cyber security awareness and skills among the younger generation. The findings from this study encourage further

development of similar programs that can be adapted and expanded to reach a wider range of participants.

REFERENCES

1. Alif, MS, & Pratama, AR (2021). Analysis of security awareness among E-Wallet users in Indonesia. Automata, 2(1).

2. Nugroho, H., Ihsan, MN, Haryoko, A., Maarif, F., & Alifah, F. (2023). Digital Security Education to Increase Public Awareness of Phishing Links. Alahyan Journal of Multidisciplinary Community Service, 1(2), 104-111.

3. Saputra, AF, Soesanto, E., Alifianto, MF, & Prastiwi, DC (2024). THE EFFECT OF CYBER SECURITY ON THE MENTAL HEALTH OF PSYCHOLOGY STUDENTS. JIP: Journal of Educational Sciences, 2(1), 12-19.

4. Tandirerung, VA, & Mangesa, RT (2023). Introduction to Cyber Security for High School Students. TECHNOVOCATION: Journal of Community Service, 89-94.

5. Yuliana, Y. (2022). The Importance of Internet Precautions for the Mental Health of Children and Adolescents. Indonesian Journal of Medical Sciences, 2(1), 25-31.

6. Yustisia, KK, Winarsih, AD, Lailiyah, M., Yudhawardhana, AN, Binatoro, AS, & Arifah, Q. (2023). Educating Elementary School Students' Digital Literacy About Cyber Security and Management Strategies. GERVASI: Journal of Community Service, 7(1), 135-147.